View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Journal of Combinatorial Theory, Series A 118 (2011) 908–919

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Finiteness of circulant weighing matrices of fixed weight

Ka Hin Leung [a], Bernhard Schmidt [b]

[a] Department of Mathematics, National University of Singapore, Kent Ridge, Singapore 119260, Republic of Singapore
[b] Division of Mathematical Sciences, School of Physical & Mathematical Sciences, Nanyang Technological University, Singapore 637371, Republic of Singapore

ARTICLE INFO

Article history:
Received 4 February 2010
Available online 28 October 2010

Keywords:
Circulant weighing matrices
Field descent
Orthogonal families

ABSTRACT

Let n be a fixed positive integer. Every circulant weighing matrix of weight n arises from what we call an irreducible orthogonal family of weight n. We show that the number of irreducible orthogonal families of weight n is finite and thus obtain a finite algorithm for classifying all circulant weighing matrices of weight n. We also show that, for every odd prime power q, there are at most finitely many proper circulant weighing matrices of weight q.

© 2010 Elsevier Inc. All rights reserved.

1. Introduction

A **circulant weighing matrix of order v** is a square matrix of the form

$$M = \begin{pmatrix} a_1 & a_2 & \cdots & a_v \\ a_v & a_1 & \cdots & a_{v-1} \\ \cdots & \cdots & \cdots & \cdots \\ a_2 & a_3 & \cdots & a_1 \end{pmatrix}$$

with $a_i \in \{-1, 0, 1\}$ for all i and $MM^T = nI$ where n is a positive integer and I is the identity matrix. The integer n is called the *weight* of the matrix.

To study circulant weighing matrices, it is very convenient to use the group ring language. Let C_v denote the cyclic group of order v, and let g be a generator of C_v. A circulant matrix M as above satisfies $MM^T = nI$ if and only if $XX^{(-1)} = n$ where X is the element of the group ring $\mathbb{Z}[C_v]$ defined by $X = \sum_{i=1}^{v} a_i g^i$ and $X^{(-1)} = \sum_{i=1}^{v} a_i g^{-i}$. Thus a circulant weighing matrix of order v and weight n is equivalent to an element X of $\mathbb{Z}[C_v]$ with coefficients $-1, 0, 1$ only satisfying $XX^{(-1)} = n$. This is the formulation we will use in the rest of our paper. Note that the weight of a circulant weighing matrix must be a square as $|\sum a_i|^2 = n$.

E-mail address: bernhard@ntu.edu.sg (B. Schmidt).

0097-3165/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jcta.2010.10.004

The existence and structure of circulant weighing matrices have been studied intensively, see [2] for a survey, [16] for many related results, and [13] for more background on weighing matrices in general. The known infinite families of circulant weighing matrices can be found in [3,10,15] and the sporadic examples in [2,4]. The *spectrum* of circulant weighing matrices of fixed weight n, i.e. the set of positive integers v such that a circulant weighing matrix of weight n exists, has been determined for $n = 4$ [11], $n = 9$ [1,19], and $n = 16$ [4,5,12].

In the present paper, we study the problem of classifying all circulant weighing matrices of fixed weight. A substantial difficulty arising with this challenging undertaking is the surprisingly nontrivial question when two such matrices should be viewed as "equivalent". The notion of "irreducible orthogonal families" we introduce in this paper answers this question.

A usual, but only partially satisfactory, approach is to restrict the attention to "proper" circulant weighing matrices. A circulant weighing matrix $X \in \mathbb{Z}[C_v]$ is called *proper* if there is no $g \in C_v$ and no proper subgroup U of C_v such that $Xg \in \mathbb{Z}[U]$.

For some cases, the notion of properness is an appropriate base for the classification of circulant weighing matrices: We will show that for every fixed odd prime power n, there are only finitely many proper circulant weighing matrices of weight n. However, such a result cannot be true in general. For instance, let $v = 2p$ where p is an odd prime. Let g respectively h be elements of C_v of order 2 respectively p. Then $X = 1 + g + h - gh$ is a proper circulant weighing matrix of weight 4. Thus there are infinitely many distinct proper circulant weighing matrices of weight 4. But of course these weighing matrices are "equivalent" in some sense and an attempted classification of circulant weighing matrices of fixed weight should reflect this. In fact, all these weighing matrices arise from the same "irreducible orthogonal family" $(\{1 + g, 1 - g\})$, a notion we introduce in this paper.

We will show that for every fixed weight n there are only finitely many irreducible orthogonal families that can give rise to circulant weighing matrices of weight n and that every circulant weighing matrix of weight n can be constructed in this way. This shows that, for any fixed n, there is a finite algorithm for finding all circulant weighing matrices of weight n. Hence we provide a quite satisfactory framework for the classification of these matrices. The proof relies on a theorem of Dirichlet on Diophantine Approximation [8, Theorem 1, p. 13] and the field descent method [17,18].

It should be mentioned that there is a close connection between the "orthogonal families" used in the present paper and the notion of "building sets" introduced in the groundbreaking paper of Davis and Jedwab [9]. In fact, if we extend the notion of orthogonal families used in our paper from cyclic to abelian groups, a major result of Davis and Jedwab can be phrased as a recursive construction of orthogonal families over abelian groups. Though the result of Davis and Jedwab only concerns abelian groups of relatively low exponent, the appearance of orthogonal families in the classification of circulant weighing matrices shows that their main idea is relevant even for cyclic groups!

2. Main results

By C_v we denote the cyclic group of order v. For a divisor w of v, we identify the subgroup of order w of C_v with C_w.

Definition 2.1. Let v be a positive integer, let w be a divisor of v, and let g be a generator of C_v. Every $X \in \mathbb{Z}[C_v]$ can be uniquely written in the form

$$X = \sum_{i=0}^{v/w-1} X_i g^i \quad \text{with } X_i \in \mathbb{Z}[C_w].$$

If $X_i X_j = 0$ for all $i \neq j$, then we say that X is *orthogonal over* C_w. We say that a subset S of $\mathbb{Z}[C_v]$ is *orthogonal over* C_w if every element of S is orthogonal over C_w.

Definition 2.2. Let v be a positive integer, and let $\mathcal{B} = \{A_1, \ldots, A_k\}$ be a finite set of elements of $\mathbb{Z}[C_v]$ with $A_i \neq 0$ for all i. We call $\mathcal{B}$ an *orthogonal family over* C_v if $A_i A_j = 0$ for all $i \neq j$. We call $\mathcal{B}$ *reducible* if there is a proper divisor w of v such that $\mathcal{B}$ is orthogonal over C_w and *irreducible* otherwise. If $\sum_{i=1}^{k} A_i A_i^{(-1)} = n$ where n is an integer, we say that $\mathcal{B}$ has *weight* n.

Definition 2.3. Let v be a positive integer, let w be divisor of v, and let $\mathcal{B} = \{A_1, \ldots, A_k\}$ be an orthogonal family over C_w. We say that $X \in \mathbb{Z}[C_v]$ *is a coset combination of* $\mathcal{B}$ if

$$X = \sum_{i=1}^{k} A_i g_i$$

where $g_1, \ldots, g_k$ are representatives of distinct cosets of C_w in C_v.

The following is the main result of this paper. It shows that, for fixed n, all circulant weighing matrices of weight n can be determined by a finite algorithm.

Theorem 2.4. *Let n be a fixed positive integer.*

(a) *There is a positive integer T, only depending on n, such that every circulant weighing matrix of weight n is a coset combination of an irreducible orthogonal family of weight n over C_v for some divisor v of T.*
(b) *The number of irreducible orthogonal families of weight n is finite, and they can be enumerated by a finite algorithm.*

In the case where the weight is an odd prime power, we can go much further. To formulate our result in this case we need some more terminology.

Definition 2.5. Let $\mathcal{B} = \{A_1, \ldots, A_k\}$ be an orthogonal family over C_v (recall that this requires $A_i \neq 0$ for all i). We call $\mathcal{B}$ *nontrivial* if $k \geqslant 2$. We say that $\mathcal{B}$ *has coefficients* $-1, 0, 1$ if all A_i have coefficients $-1, 0, 1$ only.

Theorem 2.6. *There is no nontrivial orthogonal family with coefficients $-1, 0, 1$ of odd prime power weight.*

Corollary 2.7. *Let n be an odd prime power. Then there are at most finitely many proper circulant weighing matrices of n.*

3. Preliminaries

In this section, we introduce some notation and basic facts we need in the rest of paper. For a positive integer t, we write $\zeta_t = \exp(2\pi i/t)$. Let G be a finite abelian group. We write $\circ(g)$ for the order of an element g of G. Let R be a ring. We will always identify a subset A of G with the element $\sum_{g\in A} g$ of the group ring $R[G]$. For $B = \sum_{g\in G} b_g g \in R[G]$ and an integer t we write $B^{(t)} := \sum_{g\in G} b_g g^t$ and $|B| := \sum_{g\in G} b_g$. The elements b_g are called the *coefficients* of B. We call $\{g \in G\colon\ b_g \neq 0\}$ the *support* of B. A group homomorphism $G \to H$ is always assumed to be extended to a homomorphism $R[G] \to R[H]$ by linearity.

We denote the group of complex characters of G by G^*. The character sending all elements of G to 1 is called *trivial*. For a subgroup W of G, we write $W^\perp$ for the subgroup of G^* consisting of all characters which are trivial on W. Let n be a positive integer and let m be a divisor of n. Recall that we identify the subgroup of order w of C_v with C_w. Thus $C_w^\perp$, respectively C_w^*, denotes the subgroup of C_v^* of order v/w, respectively w.

We repeatedly will make use of the following elementary properties of characters of finite abelian groups. For a proof, see [7, Section VI.3].

Result 3.1. Let G be a finite abelian group.

(a) Let $D = \sum_{g\in G} d_g g \in \mathbb{C}[G]$. Then

$$d_g = \frac{1}{|G|} \sum_{\chi\in G^*} \chi\left(Dg^{-1}\right)$$

for all $g \in G$ (Fourier Inversion Formula). In particular, two elements of $\mathbb{C}[G]$ are equal if and only if all their character values are equal.

(b) (Orthogonality relations) Let U be a subgroup of G. If $\chi \in G^*$ is nontrivial on U, then $\chi(U) = 0$. If $g \in G \setminus U$, then $\sum_{\chi \in U^\perp} \chi(g) = 0$.

(c) If H is a subgroup of G and $A, B \in \mathbb{Z}[G]$ with $\chi(A) = \chi(B)$ for all $\chi \in G^* \setminus H^\perp$, then $A = B + XH$ for some $X \in \mathbb{Z}[G]$.

Lemma 3.2. *Let G be a finite abelian group and $D = \sum a_g g \in \mathbb{Z}[G]$. For a subset S of G write $D \cap S := \sum_{g \in S} a_g g$. Let U be a subgroup of G and $h \in G$. Let χ be any character of G. Then*

$$\chi(D \cap Uh) = \frac{\chi(h)}{|U^\perp|} \sum_{\tau \in U^\perp} \chi\tau\left(Dh^{-1}\right)$$

(here $\chi\tau$ is the character which sends $g \in G$ to $\chi(g)\tau(g)$).

Proof. Using the orthogonality relations, we compute

$$\begin{aligned}
\sum_{\tau \in U^\perp} \chi\tau\left(Dh^{-1}\right) &= \sum_{\tau \in U^\perp} \sum_{g \in G} a_g \chi\tau\left(gh^{-1}\right) \\
&= \sum_{g \in G} a_g \chi\left(gh^{-1}\right) \sum_{\tau \in U^\perp} \tau\left(gh^{-1}\right) \\
&= \left|U^\perp\right| \sum_{gh^{-1} \in U} a_g \chi\left(gh^{-1}\right) \\
&= \chi(h)^{-1} \left|U^\perp\right| \sum_{k \in Uh} a_k \chi(k) \\
&= \chi(h)^{-1} \left|U^\perp\right| \chi(D \cap Uh).
\end{aligned}$$

This proves the lemma. □

For a prime p and a positive integer t let $\nu_p(t)$ be defined by $p^{\nu_p(t)} \parallel t$, i.e. $p^{\nu_p(t)}$ is the highest power of p dividing t. By $\mathcal{D}(t)$ we denote the set of prime divisors of t. The following definition is necessary for the field descent method [17] which we will use in the next section.

Definition 3.3. Let m, n be integers greater than 1. For $q \in \mathcal{D}(n)$ let

$$m_q := \begin{cases} \prod_{p \in \mathcal{D}(m) \setminus \{q\}} p & \text{if } m \text{ is odd or } q = 2, \\ 4 \prod_{p \in \mathcal{D}(m) \setminus \{2,q\}} p & \text{otherwise.} \end{cases}$$

Set

$$b(2, m, n) = \max_{q \in \mathcal{D}(n) \setminus \{2\}} \left\{ \nu_2\left(q^2 - 1\right) + \nu_2\left(\operatorname{ord}_{m_q}(q)\right) - 1 \right\}$$

and

$$b(r, m, n) = \max_{q \in \mathcal{D}(n) \setminus \{r\}} \left\{ \nu_r\left(q^{r-1} - 1\right) + \nu_r\left(\operatorname{ord}_{m_q}(q)\right) \right\}$$

for primes $r > 2$ with the convention that $b(2, m, n) = 2$ if $\mathcal{D}(n) = \{2\}$ and $b(r, m, n) = 1$ if $\mathcal{D}(n) = \{r\}$. We define

$$F(m, n) := \gcd\left(m, \prod_{p \in \mathcal{D}(m)} p^{b(p,m,n)}\right).$$

Note that $F(m,n)$ and m have the same prime divisors since b_i is positive for all i. The following basic property of $F(m,n)$ follows directly from the definition.

Result 3.4. Let n be a positive integer, let P be a finite set of primes, and let Q be the set of all positive integers which are products of powers of primes in P. Then there is an efficiently computable constant positive integer $C(P,n)$, only depending on P and n, such that $F(m,n)$ divides $C(P,n)$ for all $m \in Q$.

The following result was proved in [17].

Result 3.5 *(Field descent).* Assume $X\overline{X} = n$ for $X \in \mathbb{Z}[\zeta_m]$ where n and m are positive integers. Then

$$X\xi_m^j \in \mathbb{Z}[\xi_{F(m,n)}]$$

for some j.

The following is a special case of [14, Theorem B] (take $n = p^b$).

Result 3.6. Let p be an odd prime, and let r and w be positive integers with $(p,w) = 1$. Let $G = \langle\alpha\rangle \times H$ where $\circ(\alpha) = p^r$ and H is an abelian group of order w. Write $\beta = \alpha^{p^{r-1}}$. Let $P = \langle\beta\rangle$ be the subgroup of G of order p. Let t be a primitive root modulo p. Suppose D is an element of $\mathbb{Z}[G]$ such that $|\chi(D)|^2 = p^b$ for all $\chi \in G^* \setminus P^\perp$ where b is a positive integer.

Then there are $g \in H$ with $\circ(g)|(p-1)$, $h \in G$, $\epsilon \in \{0,1\}$, $X \in \mathbb{Z}[G]$, and $E \in \mathbb{Z}[H]$ such that

$$Dh = E\sum_{i=1}^{p-1}(\epsilon g)^i \beta^{t^i} + PX.$$

4. Proof of Theorem 2.4

As a first step towards the proof of Theorem 2.4, the following result essentially allows us to get rid of all "large" prime divisors of v.

Theorem 4.1. *Let p be a prime, and let $v = p^a w$ where a and w are positive integers with $(p,w) = 1$. Let n be a positive integer and suppose that $A \in \mathbb{Z}[C_v]$ satisfies*

$$\left|\chi(A)\right|^2 \in \{0,n\} \tag{1}$$

for all $\chi \in C_v^*$. If $p > 4^n + 1$, then A is orthogonal over C_w.

Proof. Let g be an element of C_v of order p^a. Write

$$A = \sum_{i=1}^{s} A_i g^{a_i} \tag{2}$$

where $A_i \in \mathbb{Z}[C_w]$ and the a_i are distinct elements of $\{0,1,\ldots,p^a-1\}$. By the Fourier inversion formula and (1), the coefficient of 1 in $AA^{(-1)}$ is

$$\frac{1}{v}\sum_{\chi\in C_v^*}\left|\chi(A)\right|^2 \leqslant n.$$

Since coefficient of 1 in $AA^{(-1)}$ is equal to the sum of the squares of the coefficients of A, we can assume $s \leqslant n$.

Now let τ be any complex character of C_w. It suffices to show that there is at most one i with $\tau(A_i) \neq 0$. Let χ be the extension of τ to C_v defined by $\chi(g) = \beta$ where β is a primitive p^ath root of unity. By (2), we have

$$\chi(A) = \sum_{i=1}^{s} \chi(A_i)\beta^{a_i}. \tag{3}$$

By removing all terms with $\chi(A_i) = 0$, if necessary, we can assume $\chi(A_i) \neq 0$ for all i. From (1) and (3), we get

$$\delta n = \left|\chi(A)\right|^2 = \sum_{i,j=1}^{s} \chi(A_i)\overline{\chi(A_j)}\beta^{a_i - a_j} \tag{4}$$

with $\delta \in \{0, 1\}$. Let $\rho : \mathbb{Z}[\zeta_w][C_{p^a}] \to \mathbb{Z}[\zeta_{wp^a}]$ be the epimorphism defined by $\rho(\zeta_w) = \zeta_w$ and $\rho(g) = \beta$. Note that the kernel of ρ is

$$\left\{XP\colon\ X \in \mathbb{Z}[\zeta_w][C_{p^a}]\right\}$$

where P is the subgroup of C_{p^a} of order p. Taking preimages under ρ in (4), we get

$$\delta n + XP = \sum_{i,j=1}^{s} \chi(A_i)\overline{\chi(A_j)}g^{a_i - a_j} \tag{5}$$

where $X \in \mathbb{Z}[\zeta_w][C_{p^a}]$. Note that the right-hand side of (5) has at most $n^2 - n + 1$ nonzero coefficients since $s \leqslant n$. However, if $XP \neq 0$, then the left-hand side of (5) has at least $p - 1$ nonzero coefficients. This is a contradiction, since, by assumption, $p - 1 > 4^n > n^2 - n + 1$. Hence $XP = 0$ and thus

$$\delta n = \sum_{i,j=1}^{s} \chi(A_i)\overline{\chi(A_j)}g^{a_i - a_j}. \tag{6}$$

Now assume $s \geqslant 2$. By [8, Theorem 1, p. 13] there are a positive integer $t < p$, integers b_i and real numbers ϵ_i with $|\epsilon_i| \leqslant (p-1)^{-1/s}$ such that

$$\frac{ta_i}{p} = b_i + \epsilon_i, \quad i = 1, \ldots, s. \tag{7}$$

Since $s \leqslant n$ and $p > 4^n + 1$, we conclude $|\epsilon_i| < 1/4$ for all i. Write $c_i = ta_i$ and $e_i = \epsilon_i p$. Note $|e_i| < p/4$ and that (7) implies that e_i is an integer for all i. From (7) we obtain

$$c_i \equiv e_i \mod p. \tag{8}$$

Let e_x be the largest and e_y the smallest e_i. Since $|e_i| < p/4$ for all i, we conclude

$$c_x - c_y \not\equiv c_i - c_j \mod p \tag{9}$$

for all pairs $(i, j) \neq (x, y)$. Applying the isomorphism of $\mathbb{Z}[\zeta_w][C_{p^a}]$ defined by $g \mapsto g^t$ and $\zeta_w \mapsto \zeta_w$ to (6) we get

$$\delta n = \sum_{i,j=1}^{s} \chi(A_i)\overline{\chi(A_j)}g^{c_i - c_j}. \tag{10}$$

Since $\chi(A_i) \neq 0$ for all i, and the difference $c_x - c_y$ occurs only once mod p, the coefficient of $g^{c_x - c_y}$ on the right-hand side of (10) is nonzero. But this contradicts (10). Hence $s \leqslant 1$, and, since $\tau(A_i) = \chi(A_i)$ for all i, this shows that there is at most one i with $\tau(A_i) \neq 0$. □

Lemma 4.2. *Let $v = wp^a$ where p is a prime and $a \geqslant 2$, $w \geqslant 1$ are integers. Let b be an integer with $1 \leqslant b < a$, and let $X = \sum_{i=0}^{p^{a-b}-1} X_i \zeta_{p^a}^i$ where $X_i \in \mathbb{Z}[\zeta_{wp^b}]$. If more than one X_i is nonzero, then there is no root of unity η such that $X\eta \in \mathbb{Z}[\zeta_{wp^b}]$.*

Proof. This follows from the well-known fact that $\{1, \zeta_{p^a}, \ldots, \zeta_{p^a}^{p^{a-b}-1}\}$ is independent over $\mathbb{Q}(\zeta_{wp^b})$. □

The following result shows how to make use of the field descent to show that certain group ring elements are orthogonal over rather "small" subgroups.

Theorem 4.3. *Let $v = w\prod_{i=1}^r p_i^{a_i}$ where the a_i's and w are positive integers and the p_i's are distinct primes coprime to w. Let $b_i \leqslant a_i$ be positive integers, write $k = \prod_{i=1}^r p_i^{b_i}$. Suppose that $X \in \mathbb{Z}[C_v]$ with the property for every $\tau \in C_v^*$ there is a root of unity $\eta(\tau)$ with*

$$\eta(\tau)\tau(X) \in \mathbb{Z}[\zeta_{wk}]. \tag{11}$$

Furthermore, assume that $|\tau(X)|^2 \leqslant n$ for all $\tau \in C_v^*$ for some constant n. Write $k' = w\prod_{i=1}^r p_i^{c_i}$ where

$$c_i = \begin{cases} \min\{a_i, b_i + \log n/\log p_i\} & \text{if } \log n/\log p_i \text{ is an integer, and} \\ \min\{a_i, \lceil b_i - 1 + \log n/\log p_i\rceil\} & \text{otherwise.} \end{cases}$$

Then X is orthogonal over $C_{k'}$.

Proof. We first deal with the case $r = 1$. For convenience, we drop the subscript, i.e. we write $a = a_1$, $b = b_1$, etc. Note that c is integer with $1 \leqslant c \leqslant a$. Write

$$X = \sum_{j=0}^{p^{a-c}-1} X_j h^j \tag{12}$$

where $X_j \in \mathbb{Z}[C_{wp^c}]$ and h is an element of C_v of order p^a. We have to show $X_jX_k = 0$ for all $j \neq k$. If $a = c$, there is nothing to show, so we can assume $c < a$. For any character χ of $C_{p^c w}$, we denote an extension of χ to C_v by χ'.

First, we consider the case when p^b divides the order of χ. Then the order of χ' is divisible by p^{a+b-c}. Hence $\chi'(h) = \xi$ where ξ is a primitive p^{a-c+f}th root of unity for some f with $b \leqslant f \leqslant c$. From (12) we get

$$\chi'(X) = \sum_{j=0}^{p^{a-c}-1} \chi(X_j)\xi^j \tag{13}$$

with $\chi(X_j) \in \mathbb{Z}[\zeta_{wp^f}]$. Now assume that $\chi(X_j) \neq 0$ for at least two values of j. Then by (13) and Lemma 4.2, we conclude that there is no root of unity η with $\eta\chi(X) \in \mathbb{Z}[\zeta_{wp^f}]$. But since $f \geqslant b$, this contradicts (11). Hence $\chi(X_j) \neq 0$ for all most one j. In particular,

$$\chi(X_jX_k) = 0 \tag{14}$$

for $j \neq k$ if p^b divides the order of χ.

Next, we consider the case p^b does not divide the order of χ. Note that the number of such characters $\chi \in C_{wp^c}^*$ is wp^{b-1}. Since $|\chi'(X)| \leqslant \sqrt{n}$ for all characters χ' of C_v, we conclude from Lemma 3.2 that

$$\big|\chi(X_j)\big| \leqslant \sqrt{n}. \tag{15}$$

Write $X_jX_k = \sum_{g\in C_{wp^c}} a_g g$ with $a_g \in \mathbb{Z}$. If $X_jX_k \neq 0$, then there is a g with $a_g \neq 0$. By (14), (15) and

the inversion formula,

$$1 \leqslant |a_g| \leqslant \frac{nwp^{b-1}}{wp^c} = np^{b-c-1}. \tag{16}$$

Since $a > c$, we have $c > b - 1 + \log n/\log p$ by the definition of c. Hence $p^{c-b+1} > n$, contradicting (16). This concludes the proof for the case $r = 1$.

For the proof of the general statement, we observe that each X_j from (12) also satisfies the conditions in the lemma. We can now apply induction to get the desired result. □

Definition 4.4. Let n be a positive integer, let $\{p_1, \ldots, p_r\}$ be the set of all primes $\leqslant 4^n + 1$, and let $P = \prod_{i=1}^r p_i$. Let the constant $C(P, n)$ be as defined in Result 3.4 and write $C(P, n) = \prod_{i=1}^r p_i^{b_i}$. For each i, let c_i be smallest positive integer with $p^{c_i - b_i + 1} > n$. We define

$$T(n) = \prod_{i=1}^{r} p_i^{c_i}.$$

Theorem 4.5. *Let n and v be a positive integers, and let $X \in \mathbb{Z}[C_v]$ such that $|\chi(X)|^2 \in \{0, n\}$ for all characters χ of G. Then X is orthogonal over C_d where $d = \gcd(T(n), v)$.*

Proof. Let $\{p_1, \ldots, p_r\}$ be the set of all primes $\leqslant 4^n + 1$. By Theorem 4.1 there is a divisor z of v of the form

$$z = \prod_{i=1}^{r} p_i^{a_i}, \quad a_i \geqslant 0,$$

such that X is orthogonal over C_z. Thus we can write $X = \sum_{i=0}^{v/z-1} X_i g^i$ where g is a generator of C_v, $X_i \in \mathbb{Z}[C_z]$ and the set of X_i's is an orthogonal family over C_z. Hence, for all characters $\chi \in C_v^*$, we have $\chi(X) = \chi(X_i)\chi(g^i)$ for some i. Therefore, $\chi(X)\chi(g^{-i}) \in \mathbb{Z}[\zeta_z]$. As $|\chi(X)|^2 \in \{0, n\}$, it follows that $|\chi(X_i)|^2 \in \{0, n\}$ for all i.

By Result 3.4, $F(z, n)$ divides $C(P, n)$. Hence, up to multiplication with a root of unity, $\chi(X_i) \in \mathbb{Z}[\zeta_{C(P,n)}]$ for all characters χ of C_z by Result 3.5. Hence, as $|\chi(X_i)|^2 \in \{0, n\}$ for all $\chi \in C_z^*$ and in view of Definition 4.4, Lemma 4.3 shows that each X_i is orthogonal over $C_{d'}$ where $d' = \gcd(T(n), z)$. Since $X = \sum_{i=0}^{v/z-1} X_i g^i$, this implies that X is orthogonal over C_d. □

Proof of Theorem 2.4. Let v and n be positive integers and let $X \in \mathbb{Z}[C_v]$ be a circulant weighing matrix of weight n. Let d be the smallest divisor of v such that X is orthogonal over C_d. Then $X = \sum_{i=0}^{v/d-1} X_i g^i$ where $X_i \in C_d$, and g is a generator of C_v and $X_i X_j = 0$ for all $i \neq j$. Let t be the number of nonzero X_i, $i = 0, \ldots, v/d - 1$. There are integers $a_1, \ldots, a_t$ such that $X = \sum_{i=1}^t X_{a_i} g^{a_i}$. Furthermore, for every proper divisor w of d, there is at least one X_{a_i}, $i \in \{1, \ldots, t\}$, which is not orthogonal over C_w (otherwise X would be orthogonal over C_w in contradiction to the minimality of d). Hence $\mathcal{B} = \{X_{a_1}, \ldots, X_{a_t}\}$ is an irreducible orthogonal family and X is a coset combination of $\mathcal{B}$.

If d did not divide $T(n)$, then all X_{a_i} would be orthogonal over C_w for some proper divisor w of d by Theorem 4.5, a contradiction to the irreducibility of $\mathcal{B}$. Hence d divides $T(n)$. This proves part (a) of Theorem 2.4.

For the proof of part (b), let $\{X_1, \ldots, X_t\}$, $X_i \in \mathbb{Z}[C_v]$, be an irreducible orthogonal family of weight n. Then v divides $T(n)$ by the same argument as above.

Recall that $\sum_{i=1}^t X_i X_i^{(-1)} = n$ by the definition of an orthogonal family of weight n. Since the coefficient of 1 in $X_i X_i^{(-1)}$ is at least 1, this implies $t \leqslant n$. Furthermore, the coefficients of all X_i cannot exceed $\sqrt{n}$ in absolute value.

For every divisor v of $T(n)$, there are only finitely many t-subsets of $\mathbb{Z}[C_v]$ with $t \leqslant n$ and all coefficients bounded in absolute value by $\sqrt{n}$. Since $T(n)$ has only finitely many divisors, this implies that there are only finitely many irreducible orthogonal families of weight n, and they can be enumerated in finitely many steps by brute force. This concludes the proof of Theorem 2.4. □

5. Some necessary conditions on orthogonal families

Lemma 5.1. *Let v and n be positive integers. If an orthogonal family over C_v of weight n exists, then n is a square.*

Proof. Let $\{A_1, \dots, A_k\}$ be an orthogonal family over C_v of weight n. Let χ_0 be the trivial character of C_v. Then there is j with $|\chi_0(A_j)|^2 = n$ and $\chi_0(A_j)$ is an integer. □

Definition 5.2. Let v be a positive integer, and let $\mathcal{B} = \{A_1, \dots, A_k\}$ be an orthogonal family over C_v. Let C_v^* denote the group of complex characters of C_v. We define

$$\mathcal{A}_i = \left\{\chi \in C_v^*\colon\ \chi(X_i) \neq 0\right\}$$

for $i = 1, \dots, k$.

Remark 5.3. If $\chi \in \mathcal{A}_i$, then $\chi^t \in \mathcal{A}_i$ for any t relatively prime to v.

Lemma 5.4. *Let $\mathcal{B} = \{A_1, \dots, A_k\}$ be an orthogonal family over C_v of weight n and let $\mathcal{A}_i$ be defined as above. Then each $\mathcal{A}_i$ is a union of $C_{(v,n)}^{\perp}$-cosets.*

Proof. Let p be a prime divisor of v and write $v = p^r w$ with $(p, w) = 1$. Let $\chi, \tau \in C_v^*$ such that $(p, \circ(\chi)) = 1$ and $\circ(\tau)$ is a p-power that divides $v/(n, v)$.

Claim. *If $\chi \in \mathcal{A}_i$ then $\chi\tau \in \mathcal{A}_i$.*

Assume the contrary, i.e., $\chi \in \mathcal{A}_i$ and $\chi\tau \notin \mathcal{A}_i$. Write $C_v = \langle g\rangle \times \langle h\rangle$ where g has order p^r and h has order w. Let $\rho : \mathbb{Z}[C_v] \to \mathbb{Z}[\zeta_w][C_{p^r}]$ be the homomorphism defined by $\rho(g) = g$ and $\rho(h) = \chi(h)$. Note that

$$\gamma\chi = \gamma \circ \rho \tag{17}$$

for every character γ of C_{p^r}. Write $B_j = \rho(A_j)$ for all j.

Since the A_j are an orthogonal family and in view of (17), for every $\gamma \in C_{p^r}^*$, we have $|\gamma(B_j)|^2 = n$ for one j and $\gamma(B_k) = 0$ for $k \neq j$. Let χ_0 denote the trivial character of C_{p^r}. Let τ' be the restriction of τ to C_{p^r}. Since $\chi \in \mathcal{A}_i$ and $\chi\tau \notin \mathcal{A}_i$, we have $|\chi_0(B_i)|^2 = n$ and $\tau'(B_i) = 0$. Hence there is a $k \neq i$ such that $\chi_0(B_k) = 0$ and $|\tau'(B_k)|^2 = n$. Let T be the set of characters γ of C_{p^r} with $|\gamma(B_k)|^2 = n$. Note that, by Remark 5.3, T is a union of sets M_s where M_s is the set of elements of $C_{p^r}^*$ of order p^s. By the inversion formula, the coefficient of 1 in $B_k B_k^{(-1)}$ is

$$\frac{1}{p^r}\sum_{\gamma \in C_{p^r}^*} \left|\gamma(B_k)\right|^2 = \frac{1}{p^r}|T|n. \tag{18}$$

Since $\chi_0 \notin T$, $\tau' \in T$, and $|M_s| = p^s - p^{s-1}$ for $s \geqslant 1$, we see that $|T|$ is not divisible by $\circ(\tau) = \circ(\tau')$. As $\circ(\tau)$ divides $p^r/(n, p^r)$, we conclude that $|T|$ is not divisible by $p^r/(n, p^r)$. Thus $|T|n$ is not divisible by p^r, contradicting (18). This proves the claim.

Now write $v/(v, n) = \prod_{i=1}^{t} p_i^{a_i}$ where the p_i are distinct primes. Let ψ be any character contained in $\mathcal{A}_i$. Let Γ be the subgroup of C_v^* of order $p_1^{a_1}$. If the order of ψ is divisible by $p_1^{a_1+1}$, then $\psi\Gamma \subset \mathcal{A}_i$

by Remark 5.3. If the order of ψ is exactly divisible by p_1^t, $t \leqslant a_1$, then applying the claim with $\chi = \psi^{p_1^t}$ shows that $\psi\Gamma = \chi\Gamma \subset \mathcal{A}_i$. Hence we have $\psi\Gamma \subset \mathcal{A}_i$ in all cases. Repeating this argument proves Lemma 5.4. □

Corollary 5.5. *Let v and n be coprime positive integers. Then there is no nontrivial orthogonal family of weight n over C_v.*

Proof. Suppose that $\mathcal{B} = \{A_1, \ldots, A_k\}$ is an orthogonal family over C_v with $k \geqslant 2$. As $A_1 \neq 0$, there is $\chi \in C_v^*$ with $\chi(A_1) \neq 0$. Thus $\tau(A_1) \neq 0$ for all $\tau \in C_v^*$ by Lemma 5.4. Since $A_1 A_2 = 0$, this implies $\tau(A_2) = 0$ for all $\tau \in C_v^*$. Hence $A_2 = 0$ by Result 3.1, part (a), a contradiction. □

6. Orthogonal families of odd prime power weight

In this section, we prove Theorem 2.6 and Corollary 2.7. We need the following lemma which is a generalization of [6, Lemma 3.4].

Lemma 6.1. *Let p be an odd prime, and let r and w be positive integers with $(p, w) = 1$. Let $G = \langle\alpha\rangle \times H$ where $\circ(\alpha) = p^r$ and H is an abelian group of order w. Let P be the subgroup of G of order p. Let c be any positive integer. There is no $A \in \mathbb{Z}[G]$ with coefficients $-1, 0, 1$ only satisfying*

$$AA^{(-1)} = p^{2c} - p^{2c-1}P. \tag{19}$$

Proof. Let x_1, x_2 be the number of coefficients of A equal to 1 and -1 respectively. By (19) we have $x_1 - x_2 = |A| = 0$. Comparing the coefficient of 1 on both sides of (19) we get $x_1 + x_2 = p^{2c} - p^{2c-1}$. Hence $x_1 = p^{2c-1}(p-1)/2$. To show such an A does not exist, it suffices to show $p-1$ divides x_1. From (19) we infer

$$\begin{aligned} &\left|\chi(A)\right|^2 = p^{2c} \quad \text{if } \chi \in G^* \setminus P^\perp, \\ &\chi(A) = 0 \quad \text{if } \chi \in P^\perp. \end{aligned} \tag{20}$$

Let t be a primitive element mod p. In view of (20), Result 3.6 implies

$$Ah = E\sum_{i=1}^{p-1} (\epsilon g)^i \alpha^{t^i p^{r-1}} + PX \tag{21}$$

with $h \in G$, $E \in \mathbb{Z}[H]$, $\epsilon = \pm 1$, $g \in H$, $\circ(g) | (p-1)$, and $X \in \mathbb{Z}[G]$.

We first show $\epsilon = 1$. Suppose $\epsilon = -1$ and let χ be character of G of order p^r. Then $\chi \in H^\perp \setminus P^\perp$ and thus $x := \chi(E)$ is an integer $\chi(g) = 1$, and $\chi(P) = 0$. Hence $\chi(Ah) = x\sum_{i=1}^{p-1}(-1)^i\zeta^{t^i}$ by (21) where $\zeta = \chi(\alpha^{p^{r-1}})$ is a primitive pth root of unity. Note that $\sum_{i=1}^{p-1}(-1)^i\chi(h)^{t^i}$ is a quadratic Gauss sum of absolute value $\sqrt{p}$ [20, Lemma 6.1]. Hence $|\chi(A)|^2 = |\chi(Ah)|^2 = px^2$. But from (20) we have $|\chi(A)|^2 = p^{2c}$, a contradiction. This proves $\epsilon = 1$.

Next, we derive more information on X and E. Write $X = \sum_{f\in S} a_f f$ with $S \subset G$ and $a_f \in \mathbb{Z}$. Without loss of generality, we may assume the cosets Pf, $f \in S$, are pairwise disjoint. As the p-Sylow subgroup is cyclic, we may assume that p does not divide $\circ(f)$ if p^2 does not divide $\circ(f)$, for every $f \in S$. On the other hand, observe that p divides exactly the order of every element in the support of $E\sum g^i\alpha^{t^i p^{r-1}}$. Hence, we may assume that S and the support of $E\sum g^i\alpha^{t^i p^{r-1}}$ are disjoint. Therefore, $a_f \in \{-1, 0, 1\}$ for all $f \in S$.

Now let $\rho : G \mapsto G/P$ be the natural epimorphism and write $\bar{g} = \rho(g)$. Note that $\rho(A) = 0$ by (20) and Result 3.1, part (a). Hence we get

$$0 = \rho(A) = \frac{p-1}{o(g)}\rho(E)\langle\bar{g}\rangle + p\rho(X) \tag{22}$$

from (21). Since all nonzero coefficients of $\rho(X) = \pm 1$, it follows from (22) that either $\circ(g) = p-1$ or $\rho(X) = 0$.

If $\rho(X) = 0$, then $Ah = E(\sum_{i=1}^{p-1} g^i \alpha^{t^i p^{r-1}})$. Note that to show that x_1 is a multiple of $p-1$, it suffices to show that if $f \neq f'$ are in the support of E, then

$$\left\{ fg^i \alpha^{t^i p^{r-1}} \;\middle|\; i = 1, \ldots, p-1 \right\} \cap \left\{ f' g^i \alpha^{t^i p^{r-1}} \;\middle|\; i = 1, \ldots, p-1 \right\} = \emptyset.$$

Otherwise, we have $fg^i \alpha^{t^i p^{r-1}} = f' g^j \alpha^{t^j p^{r-1}}$ for some $1 \leqslant i, j \leqslant p-1$. Since p does not divide the $|H|$, we deduce that $\alpha^{t^i p^{r-1}} = \alpha^{t^j p^{r-1}}$. As t is primitive root modulo p, we conclude $i = j$. Therefore, $f = f'$, which is impossible.

Now, suppose $\rho(X) \neq 0$. Hence, $\circ(g) = p-1$. For any $\chi \in P^{\perp} \setminus \langle g \rangle^{\perp}$, $\chi(A) = 0$ by (20) and

$$\chi\left(\sum_{i=1}^{p-1} g^i \alpha^{t^i p^{r-1}} \right) = \frac{p-1}{o(g)} \chi\left(\langle g \rangle \right) = 0$$

by Result 3.1, part (b). Thus $\chi(PX) = 0$ by (21). Hence we have $\tau(PX) = 0$ for all $\tau \in G^* \setminus (P\langle g \rangle)^{\perp}$. By Result 3.1, part (c), we can write $PX = P\langle g \rangle Y$ for some $Y \in \mathbb{Z}[G]$. As $\circ(g) = p-1$, each $P\langle g \rangle$ coset can be partitioned into p subsets

$$f\langle g \rangle, \left\{ fg^i \alpha^{t^i p^{r-1}} \;\middle|\; i = 1, \ldots, p-1 \right\}, \ldots, \left\{ g^{p-2} fg^i \alpha^{t^i p^{r-1}} \;\middle|\; i = 1, \ldots, p-1 \right\}.$$

For each of these sets, all elements of the respective set have the same coefficient in Ah. Therefore, $p-1$ divides x_1 as well. □

Proof of Theorem 2.6. Let p be an odd prime and suppose that a nontrivial orthogonal family $\{A_1, \ldots, A_k\}$ of weight $n = p^d$ over C_v exists where d is a positive integer. By Lemma 5.1, we have $n = p^{2c}$ for some positive integer c. Write $v = p^r w$ with $(p, w) = 1$. By Corollary 5.5, we have $r \geqslant 1$.

Let τ be character of C_v of order divisible by p^r, i.e., $\tau \in C_v^* \setminus C_p^{\perp}$. Since $\{A_1, \ldots, A_k\}$ is an orthogonal family of weight n, we have $|\tau(A_j)|^2 = n$ for exactly one j and $\tau(A_k) = 0$ for $k \neq j$. W.l.o.g. we may assume $|\tau(A_1)|^2 = n$. Since $\mathcal{A}_1 = \{\chi \in C_v^* \colon \chi(A_1) \neq 0\}$ is a union of cosets of $C_{p^r}^{\perp}$ by Lemma 5.4, we conclude $\tau C_{p^r}^{\perp} \subset \mathcal{A}_1$. Thus $\psi C_{p^r}^{\perp} \subset \mathcal{A}_1$ for all $\psi \in C_w^{\perp} \setminus C_p^{\perp}$ by Remark 5.3. This implies $|\chi(A_1)|^2 = n$ for all $\chi \in C_v^* \setminus C_p^{\perp}$. Furthermore, by Result 3.6, we have

$$A_1 = T + C_p X \tag{23}$$

with $T \in \mathbb{Z}[C_{pw}]$ and $X \in \mathbb{Z}[C_v]$. Since $\{A_1, \ldots, A_k\}$ is a nontrivial orthogonal family there is $\tau \in C_p^{\perp}$ with $\tau(A_1) = 0$. Thus $\tau(T) \equiv 0 \bmod p$ by (23). Since $T \in \mathbb{Z}[C_{pw}]$ we have $\psi(T) = \tau(T)$ for all $\psi \in C_p^{\perp}$. This shows

$$\psi(T) \equiv 0 \mod p \tag{24}$$

for all characters $\psi \in C_p^{\perp}$. Let $\rho : C_v \to C_v/C_p$ be the natural epimorphism. By (24) we have $\kappa(\rho(T)) \equiv 0 \bmod p$ for all characters κ of C_v/C_p. Since $\rho(T) \in \mathbb{Z}[C_{pw}/C_p]$ and p does not divide $|C_{pw}/C_p|$, this implies $\rho(T) \equiv 0 \bmod p$ by Result 3.1, part (a). Hence, in view of (23), we have

$$\rho(A_1) \equiv 0 \mod p. \tag{25}$$

Now assume $\rho(A_1) = 0$. Then $\chi(A_1) = 0$ for all $\chi \in C_p^{\perp}$ and $|\chi(A_1)|^2 = n = p^{2c}$ for $\chi \in C_v^* \setminus C_p^{\perp}$. Hence $A_1 A_1^{(-1)} = p^{2c} - p^{2c-1} C_p$ by Result 3.1, part (a). But this is impossible by Lemma 6.1. Hence $\rho(A_1) \neq 0$.

Now let $i > 1$. Since $\chi(A_1) \neq 0$ for all $\chi \in C_v^* \setminus C_p^{\perp}$, we have $\chi(A_i) = 0$ for all these characters. This means that $\phi(A_i) = 0$ where $\phi : \mathbb{Z}[C_v] \to \mathbb{Z}[\zeta_{p^r}][C_w]$ is the homomorphism which sends a generator of C_{p^r} to ζ_{p^r} and whose restriction to C_w is the identity map. Note that the kernel of ϕ is

$\{XC_p\colon\ X \in \mathbb{Z}[C_v]\}$. Hence we have $A_i = X_i C_p$ with $X_i \in \mathbb{Z}[C_v]$. This implies

$$\rho(A_i) \equiv 0 \mod p \quad \text{for } i = 2, \ldots, k. \tag{26}$$

Since $A_i \neq 0$ and $\chi(A_i) = 0$ for all $\chi \in C_v^* \setminus C_p^\perp$, there is $\tau_i \in C_p^\perp$ with $\tau_i(A_i) \neq 0$. This shows $\rho(A_i) \neq 0$ for $i = 2, \ldots, k$.

In summary, we have shown $\rho(A_i) \equiv 0 \mod p$ and $\rho(A_i) \neq 0$ for $i = 1, \ldots, k$. Note that $\rho(A_i)/p$, $i = 1, \ldots, k$, are elements of $\mathbb{Z}[C_v/C_p]$ with coefficients $-1, 0, 1$ only since the A_i have coefficients $-1, 0, 1$ only. Hence $\{\rho(A_i)/p\colon\ i = 1, \ldots, k\}$ is an orthogonal family of weight p^{2c-2} over $\mathbb{Z}[C_v/C_p]$.

Repeating this argument, we finally obtain an orthogonal family over a cyclic group whose order is coprime to the weight of the orthogonal family. But this is impossible by Corollary 5.5. □

Proof of Corollary 2.7. Suppose $X \in \mathbb{Z}[C_v]$ is a proper circulant weighing matrix with $XX^{(-1)} = n$ where n is an odd prime power. By Theorem 2.4, X is a coset combination of an irreducible orthogonal family $\mathcal{B}$ over C_w for some divisor w of v. By Theorem 2.6, $\mathcal{B}$ has only one element, i.e., $\mathcal{B} = \{A_1\}$ with $A_1 \in \mathbb{Z}[C_w]$ and $X = A_1 g$ for some $g \in C_v$. Since X is proper, we conclude $w = v$. Hence $\{X\}$ is also an irreducible orthogonal family of weight n. Since there are at most finitely many such families by Theorem 2.4, there are also at most finitely many proper circulant weighing matrices of weight n. □

Acknowledgments

We thank the referees for their suggestions and careful reading of the manuscript.

References

[1] M.H. Ang, K.T. Arasu, S.L. Ma, Y. Strassler, Study of proper circulant weighing matrices with weight 9, Discrete Math. 308 (2008) 2802–2809.
[2] K.T. Arasu, J.F. Dillon, Perfect ternary arrays , in: Difference Sets, Sequences and Their Correlation Properties, in: NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 542, Kluwer, 1999, pp. 1–15.
[3] K.T. Arasu, J.F. Dillon, D. Jungnickel, A. Pott, The solution of the Waterloo problem, J. Combin. Theory Ser. A 71 (1995) 316–331.
[4] K.T. Arasu, K.H. Leung, S.L. Ma, A. Nabavi, D.K. Ray-Chaudhuri, Determination of all possible orders of weight 16 circulant weighing matrices, Finite Fields Appl. 12 (2006) 498–538.
[5] K.T. Arasu, K.H. Leung, S.L. Ma, A. Nabavi, D.K. Ray-Chaudhuri, Circulant weighing matrices of weight 2^{2t}, Des. Codes Cryptogr. 41 (2006) 111–123.
[6] K.T. Arasu, S.L. Ma, Some new results on circulant weighing matrices, J. Algebraic Combin. 14 (2001) 91–101.
[7] T. Beth, D. Jungnickel, H. Lenz, Design Theory, second ed., Cambridge University Press, 1999.
[8] J.W.S. Cassels, An Introduction to Diophantine Approximation, Cambridge University Press, 1957.
[9] J.A. Davis, J. Jedwab, A unifying construction of difference sets, J. Combin. Theory Ser. A 80 (1997) 13–78.
[10] P. Eades, Circulant (v, k, λ)-designs, in: Combinatorial Mathematics VII, in: Lecture Notes in Math., vol. 829, Springer, 1980, pp. 83–93.
[11] P. Eades, R.M. Hain, On circulant weighing matrices, Ars Combin. 2 (1976) 265–284.
[12] L. Epstein, The classification of circulant weighing matrices of weight 16 and odd order, M.Sc. thesis, Bar-Ilan University, 1998.
[13] C. Koukouvinos, J. Seberry, Weighing matrices and their applications, J. Statist. Plann. Inference 62 (1997) 91–101.
[14] K.H. Leung, B. Schmidt, The field descent method, Des. Codes Cryptogr. 36 (2005) 171–188.
[15] K.H. Leung, S.L. Ma, B. Schmidt, Constructions of relative difference sets with classical parameters and circulant weighing matrices, J. Combin. Theory Ser. A 99 (2002) 111–127.
[16] A. Pott, Finite Geometry and Character Theory, Lecture Notes, vol. 1601, Springer, 1995.
[17] B. Schmidt, Cyclotomic integers and finite geometry, J. Amer. Math. Soc. 12 (1999) 929–952.
[18] B. Schmidt, Characters and Cyclotomic Fields in Finite Geometry, Lecture Notes in Math., vol. 1797, Springer, 2002.
[19] Y. Strassler, The classification of circulant weighing matrices of weight 9, PhD thesis, Bar-Ilan University, 1997.
[20] L.C. Washington, Introduction to Cyclotomic Fields, Grad. Texts in Math., vol. 83, Springer, Berlin/Heidelberg/New York, 1997.